

by Tony Rybczynski, Nortel Networks

Policy Enabled Networking: What's it All About?

Article

While policy management filters have been features of routers for years, they have not been widely used. But now, with routers acquiring Quality of Service (QoS) capabilities, policy management may soon become less of an option and more of a necessity.

That's because instituting QoS complicates network operations, inasmuch as it involves mediation among various, and sometimes conflicting, network requirements. Basically, the challenge is to balance various claims on network resources, and to satisfy demands by users and network managers (and application developers) for higher levels of network security, predictability, and availability.

Tony Rybczynski (TonyRyb@nortelnetworks.com) is Director of strategic marketing and technologies in the Enterprise Solutions division of Nortel Networks. He has over 27 years experience in packet switching technology. He writes a monthly Inside Networking column for CTI magazine.

From the user's point of view, policy management is about receiving appropriate treatment from the network, which is especially important in the case of business-critical applications. From the network operator's point of view, policy management is about minimizing the complexity of end-to-end management and security. It is possible, however, to think of policy management in more general terms. For example, we could say that policy management — or policy-enabled networking — is about the allocation of network resources to best support business needs.

Reviewing Business Needs

Let's step back and examine the challenges enterprise managers face when they're obliged to accommodate users' demands while maintaining the integrity of their networks.

Security: There is a need to control which users have access to which applications. With the growth of extranets and virtual private networking, the network manager faces the difficult task of meeting internal and external security requirements while still providing easy and timely user access to network resources.

Bandwidth Utilization: Bandwidth, particularly in the wide area, is an expensive resource. Even when bandwidth may be relatively abundant and inexpensive (as in campus networks), traffic peaks and failure conditions drive the need for prioritizing bandwidth across applications.



Application Predictability: As the quest for improved price/performance drives network convergence onto unified network infrastructures, network operators find themselves with additional responsibility. That is, they need to allocate network resources to meet the needs of time-sensitive data and emerging real-time voice, video, and multimedia applications. Since not all applications are equally business critical, the network operator has to ensure that policy guidelines are established and enforced.

Administrative And Network Management Complexity: As organizations implement new applications, the number of administration systems in the network increases. As a result, the simple task (conceptually) of moves and changes becomes a nightmare across multiple configuration databases.

Satisfying Business Needs

To accommodate user demands while maintaining network integrity, network managers must find a way to bring predictability and control to business-critical applications. One way is to build networks that are automatically aware of who is trying to do what. Such networks correlate information about each user and the application being run, taking into account the security attributes of users and applications, business priorities, and the near-real-time operational state of the network.

All of this information is used to determine if the user is authorized to run the application, and if so, what priority the user should receive and how much of network resources (for example, bandwidth) should be allocated. For example, the user surfing the Internet may be given a lower priority than the person running a mission-critical application.

But how do we handle information about users and applications and network characteristics and business priorities? How do we distill all this information into resource allocation imperatives? The answer is policy management.

Policy Management

Policy management includes three fundamental functions:

- Provisioning or configuring the network switches and routers.
- Enforcement of the provisioned policies.
- Verification (or auditing) of network operation.

In more general terms, policy management is an implementation of a set of rules or policies which dictate the access and use of resources on a per user, application, or company basis to meet established business objectives. It is essentially focused on providing end-to-end QoS (bandwidth, latency, priority) and security (authentication, authorization, auditing).

Policy Management Components

As it evolves, policy management will provide the enterprise with a simple, unified solution to better meet business needs. Underneath the unified surface, however, policy management will evidence several distinct components, including advanced directories, policy servers, policy clients, and policy-enabled network elements.

Advanced Directory: An advanced directory has as its goal the consolidation and linking of disparate directories (which have typically emerged over time) into what is, in effect, a single, global directory. In such a scenario, the directory becomes a key component of the network. Policies, user information, network configuration data, and network addresses can all be found in this “central” location. The central directory must have the ability to be distributed (for avoiding the need for a megaserver), replicated (for improved performance), and partitioned (isolating more secure information).

The benefits of creating this virtual central directory (virtual in the sense that the directories are linked together to appear as one) can be significant. For example, labor costs related to administration and management may be substantially reduced.

Recognizing the significant potential benefits of unified directory services, several vendors have recently introduced directory products designed to meet the demands of policy-based networking. Some of the competing solutions include Netscape's Directory Server, Novell's Directory Service (NDS), Microsoft's Active Directory, ICL's i500 Directory, Sun Microsystems' Sun Directory Services, and Banyan Systems' Streettalk, to name just a few. While a unified directory is clearly the end point, establishing an initial directory system around some basic policy management needs is a realistic starting point.

Policy Server: The policy server is the heart of any policy management system. The policy server is responsible for gathering all of the relevant information, making a decision based on the administrator's policies, and then communicating that decision to the network via a policy transaction protocol. The goal of the policy server is to develop a response consistent with the policy, retrieving other data such as network availability or utilization, time-of-day, or service level agreement (SLA) information as appropriate. The response is transmitted to the policy enforcement device (for example, a switch/router) using a policy transaction protocol.

Policy Clients: Policy-enabled clients interact with policy servers. While an administrator sets policies at the user level, policy clients in edge devices recognize only IP addresses. Therefore, policy management is closely tied to IP address management. For example, an IP address management tool can be used to bind a user to an IP address and,

through support of the Dynamic Host Connection Protocol (DHCP), keep this address dynamically updated. With this functionality, administrators can define policies according to users or applications that they recognize, while the information is abstracted to an IP address that the edge device will recognize.

Policy-Enabled Network Elements: A policy-enabled network consisting of switches and routers not only provides transport of traffic at the required priority level, but also enforcement of the policy for that traffic. Each device along the traffic's path individually ensures that the policy is enforced locally, relying on a policy server to coordinate the end-to-end policy.

Key Enabling Technologies

Directory Enabled Networks (DEN):

The DEN initiative is an industry-wide initiative integrating directory services and networks, enabling the development of rich network applications that will operate with a variety of network and directory vendor offerings. DEN defines a way to retrieve and store information about network policies in a database. DEN software then gathers information from multiple directories and matches it with specific policies for devices, users, and applications.

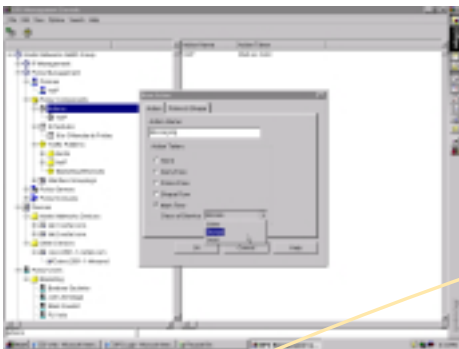
DEN becomes increasingly important as mission-critical business applications are built on general-purpose intranets, extranets, and the Internet. As these applications compete with lower priority applications such as casual Web browsing, DEN will allow prioritization of network resources for specific applications or users.

This could, for example, allow payroll data or an urgent customer order to be prioritized (in terms of bandwidth availability) over an employee accessing a Web site.

X.500 Global Directory Service: X500 is a series of standards-based protocols specifying a model for connecting multiple directory services to form one distributed global directory. Local databases hold and maintain portions of the global database, and the directory information is made available via local servers.

As such, the user perceives the entire directory to be accessible from the local server.

The X.500 directory is organized under a common root directory in a "tree" hierarchy reflecting organizational requirements. Typically, this hierarchy may be based on geographic or organizational boundaries. Each item or entry in the X.500 directory describes one object (for example, a person, a network resource, or a company). One of X.500's unique characteristics is that, as long as the X500 format is followed, locally established optional attributes are possible, permitting a flexible and more manageable solution.



Product Information

This is not part of the published article.

Optivity* Policy Services 1.0 is a system-level software application suite designed to provide application prioritization in the enterprise networking environment. A key component of the Optivity product family, Optivity Policy Services enables network managers to take a proactive approach to bandwidth management and prioritization of business-critical traffic flows across the enterprise.

Optivity Policy Services enhances customer value by delivering a simplified and pragmatic, yet comprehensive management framework for policy management. Rather than applying policies on a per-device basis, Optivity Policy Services takes a systems approach to policy configuration and deployment. Only Nortel Networks delivers a policy management framework that addresses the needs of telephony, video and data applications as an integrated system.

Lightweight Directory Access Protocol (LDAP):

LDAP is a directory access protocol whose purpose is to provide a standards-based mechanism that permits any client, server, or application to access any directory service that supports the LDAP protocol interface. The ultimate goal is to facilitate the integration of new applications making use of directory services. From PCs to networking components, LDAP will simplify and promote the deployment of directory services across enterprise networks.

Policy Transaction Protocols: The policy transaction protocol functions as the intermediary between the policy client and the policy server. It is responsible for transferring the policy request and policy response between these two nodes.

Currently, there are two protocols vying to become the IETF standard for a policy transaction protocol — COPS and DIAMETER. The Common Open Policy Service Protocol (COPS) is a simple query-and-response protocol for exchanging policy information between a policy server and its client (or clients). COPS also has the unique feature of allowing the policy control decision to be communicated between the policy client and the policy server in order to determine the validity of that decision.

DIAMETER enables communication between clients and servers for authentication, authorization, and accounting of various services. One of the unique features of DIAMETER is that it allows the policy to send unsolicited messages to its clients, permitting policy changes to be made and immediately communicated down to the policy client, improving network response times.

What's Next?

Some vendors are stepping up to the policy management challenge by developing integrated frameworks to allocate resources across multi-vendor networks. Typically, such frameworks are achieved by:

Integrating policies and service level management with existing network management capabilities. Incorporating and expanding the breadth of application intelligence features, such as QoS and security across the data networking product.

Policy management is an emerging solution set which enables business-critical networking applications to perform to specific levels for specific users. Policy management greatly facilitates the delivery of reliable, differentiated, scalable, and secure voice and data solutions.

Reprinted from CTI® magazine, volume 4, dated January 1999, published by Technology Marketing Corporation, One Technology Plaza, Norwalk, CT 06854 USA. Copyright © 1999 Technology Marketing Corporation, all rights reserved. For information about annual subscriptions, call 800-243-6002 or 203-852-6800 or visit the publication's Web site at www.ctimag.com.



<http://www.nortelnetworks.com>

*Nortel Networks, the Nortel Networks logo, the Globemark, How the World Shares Ideas, Unified Networks, and Optivity are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 1999 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document. Printed in USA.